Hyperelliptic Curves and their Jacobians

Benjamin Smith

Isogeny school, online, 2021

Inria + École polytechnique, France

Outline

Today / Class 1:

The basic geometry and arithmetic of hyperelliptic curves and their Jacobians.

Genus 2 is an important special case, but it helps to see the broader context.

Tomorrow / Class 2:

- Cryptographic aspects
- First steps in genus-2 isogeny-based cryptography

Recall...

Perfect ground fields

We work over a **perfect** field $\mathbb{k}$. This means

- Every *irreducible* polynomial over $\mathbb{k}$ has *distinct* roots in $\overline{\mathbb{k}}$
- *Equivalently*: Either $\mathrm{char}(\mathbb{k}) = 0$, or $\mathrm{char}(\mathbb{k}) = p$ and the Frobenius $\alpha \mapsto \alpha^p$ is an automorphism.

Examples:

1. Finite fields: $\mathbb{k} = \mathbb{F}_q$ *(what we're really interested in)*
2. Characteristic 0: $\mathbb{k} = \mathbb{Q}, \mathbb{Q}(\sqrt{13}), \mathbb{Q}(t), \mathbb{Q}_p, \mathbb{R}, \mathbb{C}$, ...
3. ...But not (e.g.) $\mathbb{k} = \mathbb{F}_q(t)$
   (Because $x^p - t$ is irreducible, but has one multiplicity-p root $t^{1/p}$ over $\overline{\mathbb{F}_q(t)}$). Also, $\alpha \mapsto \alpha^p$ is not an automorphism of $\mathbb{F}_q(t)$: there is no preimage of t.)

Fields of definition

A thing (a point, a set, a curve, a function) is **defined over** $\mathbb{k}$ if it is fixed by $\mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k})$.

Example: the set $\{1+\sqrt{-1}, 1-\sqrt{-1}\} \subset \mathbb{Q}(\sqrt{-1})$ is defined over $\mathbb{Q}$.

If $\mathbb{k} = \mathbb{F}_q$, then $\mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k})$ is (topologically) generated by the q-power Frobenius, so the objects defined over $\mathbb{F}_q$ are those fixed by/commuting with Frobenius.

If X is a thing, then $X(\mathbb{k})$ denotes its elements/points defined over $\mathbb{k}$.

Hyperelliptic Curves

From elliptic to hyperelliptic curves

So far, we've considered cryptosystems built from elliptic curves and their isogenies.

But what's so special about elliptic curves?

More generally: we could try working with any **algebraic curve** $\mathcal{X}$ over $\mathbb{k}$.

- $\mathcal{X} = \mathbb{P}^1 =$ a line
- $\mathcal{X} =$ an elliptic curve $\mathcal{E} : y^2 = x^3 + Ax + B$
- $\mathcal{X} : y^2 = f(x)$ with $\deg f > 4$ (hyperelliptic curves)
- ...More generally, a plane curve $\mathcal{X} : F(x, y) = 0$ in $\mathbb{A}^2$

Questions: What kinds of groups do you get? What are the analogues of isogenies?

Hyperelliptic curves:

$$\mathcal{X} : y^2 = f(x) = x^d + \cdots$$

with f squarefree, of degree $d > 4$.
(NB: $d = 1, 2 \implies$ conics; $d = 3, 4 \implies$ elliptic curves.)

Hyperelliptic involution:

$$\iota : (x, y) \longmapsto (x, -y) .$$

Key fact: $P \mapsto x(P)$ defines a double cover $\mathcal{X} \to \mathcal{X}/\langle\iota\rangle \cong \mathbb{P}^1$.

Point(s) at infinity:

odd $d \implies$ **one** point ∞ at infinity.
even $d \implies$ **two** points ∞_+, ∞_- at infinity.

The function field

If $\mathcal{X} : F(x, y) = 0$ is a plane curve over $\mathbb{k}$, then its **function field** is

$$\mathbb{k}(\mathcal{X}) = \mathbb{k}(x)[y]/(F(x, y)) .$$

Elements: rational fractions in x and y, modulo the curve equation $F(x, y) = 0$.

For more general, non-plane curves, $\mathbb{k}(\mathcal{X}) :=$ *fraction field of the coordinate ring.*

Divisors

Zeroes and Poles

Rational functions on $\mathcal{X}$ have *poles* and *zeroes*:

zeroes of f are the points P on $\mathcal{X}$ where $f(P) = 0$.

poles of f are the points P on $\mathcal{X}$ where $f(P) = \infty$.

Note: (zeroes and poles can occur with multiplicity > 1*.)*

Theorem: If f is a nonzero function in $\overline{\mathbb{k}}(\mathcal{X})$, then

1. f has only finitely many zeroes and poles, and
2. counted with multiplicity, $\#\,\mathsf{zeroes}(f) = \#\,\mathsf{poles}(f)$.

Orders of vanishing

The **order of vanishing** of a nonzero function f at a point P of $\mathcal{X}$ is

$$\mathrm{ord}_P(f) := \begin{cases} n & \text{if } f \text{ has a zero of multiplicity } n \text{ at } P \\ -n & \text{if } f \text{ has a pole of multiplicity } n \text{ at } P \\ 0 & \text{otherwise} \end{cases}$$

Useful rules:

- $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$ for all f, g, P
- $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ for all f, g, P
- $\mathrm{ord}_P(\alpha) = 0$ for all constants $\alpha \neq 0$ in $\overline{\mathbb{k}}$
- $\mathrm{ord}_P(\sum_i \alpha_i x^{a_i} y^{b_i}) = n$ if the plane curve $\sum_i \alpha_i x^{a_i} y^{b_i} = 0$ intersects $\mathcal{X}$ with multiplicity n at P

Principal divisors

Each function $f \neq 0$ on $\mathcal{X}$ has an associated **principal divisor**

$$\mathrm{div}(f) = \sum_{P \in \mathcal{X}(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(f)(P)\,.$$

The sum is **formal**: there is no addition law on the points.

1. $\mathrm{div}(f) = 0$ if and only if f is constant (in $\overline{\mathbb{k}}_q \setminus \{0\}$);
2. $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ and $\mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$;
3. $\mathrm{div}(f) = \mathrm{div}(g) \iff f = \alpha g$ for some $\alpha \neq 0$ in $\overline{\mathbb{F}}_q$.

The principal divisors form a group

Since $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, the set of principal divisors forms a **group**

$$\mathrm{Prin}(\mathcal{X}) := \left\{\mathrm{div}(f) : f \in \overline{\mathbb{k}}(\mathcal{X})\right\} .$$

Functions are determined by their principal divisors, up to constant factors.
Or, if you like exact sequences:

$$1 \longrightarrow \overline{\mathbb{k}}^{\times} \longrightarrow \overline{\mathbb{k}}(\mathcal{X})^{\times} \longrightarrow \mathrm{Prin}(\mathcal{X}) \longrightarrow 0\,.$$

Examples

Consider the elliptic curve $\mathcal{E} : y^2 = x^3 + 1$ over $\mathbb{F}_{13}$.

- $\mathrm{div}(x) = (0, 1) + (0, -1) - 2\infty$;
- $\mathrm{div}(y) = (-1, 0) + (4, 0) + (-3, 0) - 3\infty$;
- $\mathrm{div}(x^2/y) = 2(0, -1) + 2(0, 1) - (-1, 0) - (4, 0) - (-3, 0) - \infty$;
- $\mathrm{div}(\frac{x^2-y-1}{xy}) = (0, -1) + (2, 3) + \infty - (0, 1) - (-3, 0) - (4, 0)$.

More generally:
If $f(x, y) = 0$ is the line through P and Q, then $\mathrm{div}(f) = P + Q + (\ominus(P \oplus Q)) - 3\infty$.
(Here, $\oplus$ means the group law on $\mathcal{E}$, and $\ominus$ is negation.)

General divisors

Divisors on $\mathcal{X}$ are *formal sums* of points in $\mathcal{X}(\overline{\Bbbk})$ with *arbitrary* coefficients in $\mathbb{Z}$.

We define a (free abelian, infinitely generated) group

$$\mathrm{Div}(\mathcal{X}) := \Big\{ \sum_{P \in \mathcal{X}(\overline{\mathbb{F}}_q)} n_P(P) \Big\},$$

with the n_P in $\mathbb{Z}$, and only finitely many $n_P \neq 0$.

Of course, $\mathrm{Prin}(\mathcal{X})$ is a subgroup of $\mathrm{Div}(\mathcal{X})$.

The group $\mathrm{Div}(\mathcal{X})$ is way too big, and tells us nothing about the geometry of $\mathcal{X}$.

We work with the **Picard group**: the quotient

$$\mathrm{Pic}(\mathcal{X}) := \mathrm{Div}(\mathcal{X})/\mathrm{Prin}(\mathcal{X})\,.$$

Elements are **divisor classes**:

$$[D] = \{D + \mathrm{div}(f) : f \in \overline{\mathbb{k}}\}\,.$$

If D_1 and D_2 are in the same class, then we say they are *linearly equivalent*:

$$D_1 \sim D_2 \iff D_1 = D_2 + \mathrm{div}(f) \text{ for some } f \in \overline{\mathbb{k}}(\mathcal{X})\,.$$

Degree

We have a **degree** homomorphism $\mathsf{deg} : \mathrm{Div}(\mathcal{X}) \to \mathbb{Z}$,

$$\mathsf{deg}(\sum_P n_P(P)) = \sum_P n_P\,.$$

Its kernel is a subgroup of $\mathrm{Div}(\mathcal{X})$, denoted $\mathrm{Div}^0(\mathcal{X})$:

$$\mathrm{Div}^0(\mathcal{X}) := \ker \mathsf{deg} = \{D \in \mathrm{Div}(\mathcal{X}) : \mathsf{deg}(D) = 0\} \subset \mathrm{Div}(\mathcal{X})\,.$$

Every function has *the same number* of zeroes and poles, so

$$\mathrm{Prin}(\mathcal{X}) \subseteq \mathrm{Div}^0(\mathcal{X}) \quad \text{and} \quad \mathrm{Prin}(\mathcal{X})(\Bbbk) \subseteq \mathrm{Div}^0(\mathcal{X})(\Bbbk)\,.$$

The inclusion is strict for almost all curves: **not every degree-0 divisor is principal!**

Why are they called divisors?

Idea: *degree-0 divisors are "parts of functions".*

Example: Consider the elliptic curve $\mathcal{E} : y^2 = x^3 + 1$. The divisors

$$D_1 = (0, 1) - \infty \quad \text{and} \quad D_2 = (0, -1) - \infty$$

are both in $\mathrm{Div}^0(\mathcal{E})$. Neither is principal, but

$$D_1 + D_2 = \mathrm{div}(x) .$$

So we can view D_1 and D_2 as being "parts" (or even "factors") of the function x...

Degrees of divisor classes

The deg homomorphism is well-defined on divisor classes:

$$\begin{aligned} \mathsf{deg} : \mathrm{Pic}(\mathcal{X}) &\longrightarrow \mathbb{Z} \\ [D] &\longmapsto \mathsf{deg}(D) \end{aligned}$$

(since $\mathsf{deg}(\mathrm{div}(f)) = 0$ for all f).

Hence, $\mathrm{Div}^0(\mathcal{X})$ splits up into divisor classes: we set

$$\begin{aligned} \mathrm{Pic}^0(\mathcal{X}) &:= \ker(\mathsf{deg} : \mathrm{Pic}(\mathcal{X}) \to \mathbb{Z}) \\ &= \mathrm{Div}^0(\mathcal{X})/\mathrm{Prin}(\mathcal{X})\,. \end{aligned}$$

Structure of the Picard group

If we fix any "base point" P on $\mathcal{X}$, then the map $D \mapsto (D - \deg(D)\infty, \deg(D))$ defines isomorphisms

$$\mathrm{Div}(\mathcal{X}) \stackrel{\cong}{\longleftrightarrow} \mathrm{Div}^0(\mathcal{X}) \times \mathbb{Z}$$
$$\mathrm{Pic}(\mathcal{X}) \stackrel{\cong}{\longleftrightarrow} \mathrm{Pic}^0(\mathcal{X}) \times \mathbb{Z}\,.$$

The "interesting" stuff all happens in $\mathrm{Pic}^0(\mathcal{X})$, which has the structure of an **abelian variety**: a geometric object defined by polynomial equations in projective coordinates, with a polynomial group law.

(Stop and think about what this means for a minute: divisor classes can be defined by tuples of coordinates, and addition of divisor classes modulo linear equivalence defined by polynomial formulæ in those coordinates!)

Differentials

Differentials

Differentials on $\mathcal{X}$ look like gdf, where g and f are in $\Bbbk(\mathcal{X})$, with

$$g_1 df_1 = g_2 df_2 \iff \frac{g_2}{g_1} = \frac{df_1}{df_2} \quad (\leftarrow \text{usual derivative}) .$$

Differentials

- obey the usual **product rule**: $d(fg) = fdg + gdf$;
- are $\overline{\Bbbk}$**-linear**: $d(\alpha f + \beta g) = \alpha df + \beta dg$ for α, β in $\overline{\Bbbk}$;
- and **differentials of constants are zero**: $d\alpha = 0$ for α in $\overline{\Bbbk}$.

Example: on $\mathcal{E} : y^2 = x^3 + 1$, we have

$$2ydy = 3x^2dx$$

Differentials are **not functions** on $\mathcal{X}$, but they do give linear functions on the tangent spaces of $\mathcal{X}$. They are very helpful in *linearizing* problems on $\mathcal{X}$.

The space of differentials

The differentials on $\mathcal{X}$ form a one-dimensional $\overline{\mathbb{k}}(\mathcal{X})$-vector space, $\Omega(\mathcal{X})$.

That is: if we fix some differential dx, then every other differential in $\Omega(\mathcal{X})$ is equal to $f dx$ for some function f.

On the other hand: $\Omega(\mathcal{X})$ is an infinite-dimensional $\overline{\mathbb{k}}$-vector space.

Divisors of differentials

Differentials have **divisors**!

First, for each point P of $\mathcal{X}$, we fix a *local parameter* t_P near P on $\mathcal{X}$: ie any function with a simple zero at P.

If ω is a differential then ω/dt_P is a function, so we set

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\omega/dt_P)$$

(perhaps amazingly, $\mathrm{ord}_P(\omega)$ *is independent of the choice of* t_P*)* and

$$\mathrm{div}(\omega) := \sum_{P \in \mathcal{X}} \mathrm{ord}_P(\omega)(P)\,.$$

What is the divisor of dx on an elliptic curve $\mathcal{E} : y^2 = f(x)$?

At points (α, β) where $\beta \neq 0$, we can use $t_{(\alpha,\beta)} = x - \alpha$:

$$\mathrm{ord}_{(\alpha,\beta)}(dx) = \mathrm{ord}_{(\alpha,\beta)}(\frac{dx}{d(x-\alpha)}) = \mathrm{ord}_{(\alpha,\beta)}(1) = 0\,.$$

If $\beta = 0$ then $x - \alpha$ is not a local parameter at $(\alpha, 0)$ (it has a double zero), but we can use $t_{(\alpha,0)} = y$; hence

$$\mathrm{ord}_{(\alpha,0)}(dx) = \mathrm{ord}_{(\alpha,0)}(\frac{dx}{dy}) = \mathrm{ord}_{(\alpha,0)}(\frac{2y}{f'(x)}) = 1\,.$$

At infinity: we know $\mathrm{ord}_\infty(x) = -2$ and $\mathrm{ord}_\infty(y) = -3$, so we can take $t_\infty = x/y$:

$$\mathrm{ord}_\infty(dx) = \mathrm{ord}_\infty(\frac{dx}{d(x/y)}) = \mathrm{ord}_\infty(\frac{2yf(x)}{2f(x) - xf'(x)}) = -3\,.$$

Canonical divisors

Note that

$$\mathrm{div}(f\omega) = \mathrm{div}(\omega) + \mathrm{div}(f) \qquad \text{for all } f \in \overline{\Bbbk}(\mathcal{X}), \omega \in \Omega(\mathcal{X})\,.$$

So: the divisors of differentials on $\mathcal{X}$ are all in **the same divisor class**, which we call the **canonical class**, $[K]$.

Any divisor in $[K]$ is called a **canonical divisor**.

On the hyperelliptic curve $\mathcal{H} : y^2 = f(x) = \prod_{i=1}^{d}(x - \alpha_i)$, we have

$$K = \mathrm{div}(dx) = \begin{cases} \sum_{i=1}^{d}(\alpha_i, 0) - 3\infty & d \text{ odd} \\ \sum_{i=1}^{d}(\alpha_i, 0) - 2(\infty_+ + \infty_-) & d \text{ even} \end{cases}$$

Nonconstant differentials with no poles

Consider the elliptic case: if $y^2 = f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, then

$$\mathrm{div}(dx) = (\alpha_1, 0) + (\alpha_2, 0) + (\alpha_3, 0) - 3\infty\,.$$

Notice that $\mathrm{div}(y) = \mathrm{div}(dx)$, so

$$\mathrm{div}(\frac{dx}{y}) = 0\,.$$

The differential dx/y is a *nonconstant* differential with no poles (or zeroes!).

Regular differentials

We call differentials with no poles **regular differentials**.

The regular differentials on $\mathcal{X}$ form a (finite-dimensional) $\mathbb{k}$-vector space

$$\Omega^1(\mathcal{X}) = \{\omega \in \Omega(\mathcal{X}) : \omega \text{ is regular}\}\,.$$

The **genus** of $\mathcal{X}$ is defined to be the dimension of $\Omega^1(\mathcal{X})$.

Think: the genus gives a first classification of the intrinsic algebraic complexity of a curve.

Genus of hyperelliptic curves

For hyperelliptic curves

$$\mathcal{X} : y^2 = f(x) = x^d + \cdots \ ,$$

we have

$$\Omega^1(\mathcal{X}) = \left\langle \frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{\lfloor (d-1)/2-1 \rfloor}dx}{y} \right\rangle ,$$

so

$$g(\mathcal{X}) = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

Explicit regular differentials

More generally, if $\mathcal{X}/\mathbb{k}$ is a nonsingular plane curve of genus g defined by

$$\mathcal{X} : F(x, y) = 0 \ ,$$

then its regular differentials are

$$\Omega^1(\mathcal{X}) = \left\langle \frac{x^i}{(\partial F/\partial y)(x, y)} dx \right\rangle_{i=0}^{g-1} .$$

Fact: for any curve $\mathcal{X}$, we have $\deg(K) = 2g - 2$.

Riemann–Roch

Into space!

Let's get back to functions on $\mathcal{X}$.

Evaluating a single function at points maps us from $\mathcal{X}$ to $\mathbb{P}^1$
(the poles of the function map to ∞).

Evaluating a tuple $(f_1, \ldots, f_n)$ of functions gives us a map

$$P \mapsto (f_1(P) : \cdots : f_n(P) : 1) \in \mathbb{P}^n .$$

We want to control behaviour at infinity, hence the poles of the f_i.

Riemann–Roch Spaces

A divisor $D = \sum_P n_P P$ is **effective** if all of the $n_P \geq 0$. We define

$$L(D) := \{f \in \mathbb{k}(\mathcal{X}) : D + \mathrm{div}(f) \text{ is effective } \} \cup \{0\} .$$

...So $L(D)$ consists of the functions whose poles are contained in D.

$$L(D_1 + D_2) \supseteq L(D_1)L(D_2) \quad \text{for any } \textbf{effective } D_1, D_2 .$$

Note: if $\mathcal{X} = \mathbb{P}^1$, then $L(d\infty) = \{\text{polynomials of degree } \leq d\}$.

Dimension of Riemann–Roch Spaces

Fact: $L(D)$ is a finite-dimensional $\mathbb{k}$-vector space. *What is its dimension?*

- If $\deg D < 0$, then $D + \mathrm{div}(f)$ can never be effective
  $\implies \dim L(D) = 0$ when $\deg D < 0$.
- $L(0) = \mathbb{k}$ (functions with no poles are constant),
  $\implies \dim L(0) = 1$.
- More generally, $L(D) = ?$

The Riemann–Roch theorem tells us that for any D,

$$\dim L(D) - \dim L(K - D) = \deg D - g + 1\,.$$

Recall that K is (any) canonical divisor, and

$$L(K - D) \longleftrightarrow \left\{\omega \in \Omega^1(\mathcal{X}) : \omega = 0 \text{ on } D\right\}\,.$$

In particular, for “large enough” D, we have $L(K - D) = 0$ and hence $\dim L(D) = \deg D - g + 1$.

Weierstrass models of elliptic curves

Suppose $\mathcal{E}$ is an **abstract elliptic curve** over $\Bbbk$, and let $\mathcal{O} \in \mathcal{E}(\Bbbk)$.

We have $K = 0$, so Riemann–Roch gives $\dim L(D) = \deg D$ for effective D.

- $L(\mathcal{O}) = \Bbbk = \langle 1 \rangle$ (constants)
- $\dim L(2\mathcal{O}) = 2 \implies L(2\mathcal{O}) = \langle 1, x \rangle$ for some x
- $\dim L(3\mathcal{O}) = 3 \implies L(3\mathcal{O}) = \langle 1, x, y \rangle$ for some y
- $L(4\mathcal{O}) = \left\langle 1, x, x^2, y \right\rangle$
- $L(5\mathcal{O}) = \left\langle 1, x, x^2, y, xy \right\rangle$
- $L(6\mathcal{O}) = \left\langle 1, x, x^2, x^3, y, xy, y^2 \right\rangle$, but $\dim L(6\mathcal{O}) = 6$, so there must be a nontrivial linear relation between the 7 functions $1, x, x^2, x^3, y, xy, y^2$.

$\implies$ Weierstrass equation $y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6$.

$L(3\mathcal{O})$ gives us an embedding $\mathcal{E} \to \mathbb{P}^2 = \mathbb{P}(L(3\mathcal{O}))$ defined by $P \mapsto (x(P) : y(P) : 1)$ and $\mathcal{O} \mapsto \infty = (0 : 1 : 0)$.

Application: canonical models for genus 2 curves

Suppose $\mathcal{X}$ is a curve of **genus 2**.

- We have $\deg K = 2g - 2 = 2$, so $L(-nK) = 0$ for $n > 1$.
- Apply R–R to $D = 0 \implies \dim L(K) = 2$, so $L(K) = \langle 1, x \rangle$ for some x.
- Apply R–R to $D = nK$, $n > 1$: $\dim L(nK) = 2n - 1$ for $n > 1$.
- $L(2K) \supseteq \langle 1, x, x^2 \rangle$ but $\dim L(2K) = 3$, so $L(2K) = \langle 1, x, x^2 \rangle$.
- $L(3K) \supseteq \langle 1, x, x^2, x^3 \rangle$ but $\dim L(3K) = 5$, so $L(3K) = \langle 1, x, x^2, x^3, y \rangle$ for some new y
- ...$L(4K) = \langle 1, x, x^2, x^3, x^4, y, xy \rangle$
- ...$L(5K) = \langle 1, x, x^2, x^3, x^4, x^5, y, xy, x^2y \rangle$

...Every genus 2 curve is hyperelliptic

Now $L(6K) \supseteq \langle 1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^2y, x^3y, y^2 \rangle$, but R–R says $\dim L(6K) = 11$, so there is a nontrivial $\Bbbk$-linear relation between the 12 functions:

$$y^2 + \sum_{i=0}^{3}(a_i x^i y) = \sum_{i=0}^{6} b_i x^i \quad \text{with the } a_i, b_i \in \Bbbk\,.$$

$\mathrm{char}(\Bbbk) \neq 2$: replace y with $y - \frac{1}{2}\sum_{i=0}^{3} a_i x^i$ to get $y^2 = \sum_{i=0}^{6} f_i x^i$.

Now $P \mapsto (x(P), y(P))$ defines a map from $\mathcal{X}$ into the plane; its image is the hyperelliptic curve

$$\mathcal{X} : y^2 = f(x) = \sum_{i=0}^{6} f_i x^i\,.$$

Hyperelliptic Jacobians

Suppose $\mathcal{X} : y^2 = f(x)$ is hyperelliptic of genus $g > 1$.

From now on, we suppose f has odd degree,
so $\mathcal{X}$ has a single point ∞ at infinity.

Even degree case is (only) slightly more complicated.

Goal: to define a compact (and algebraic) representation for $\mathrm{Pic}^0(\mathcal{X})$.

Reduced representatives for classes

If $[D]$ is in $\mathrm{Pic}^0(\mathcal{X})$, then $[D]$ has a unique **reduced representative**:

$$[D] = [P_1 + \cdots + P_r - r\infty]$$

for some $P_1, \ldots, P_r \in \mathcal{X}$ depending on $[D]$ (not D) such that

- $P_i \neq \infty$ and $P_i \neq \iota(P_j)$ for $i \neq j$ (semi-reducedness)
- $r \leq g$ (reducedness)

$$[D] \in \mathrm{Pic}^0(\mathcal{X})(\Bbbk) \iff P_1 + \cdots + P_r \in \mathrm{Div}(\mathcal{X})(\Bbbk)$$

Note: the individual P_i need not be in $\mathcal{X}(\Bbbk)$!

Why?

Riemann–Roch guarantees the existence of the reduced representative.

If $[D]$ is in $\mathrm{Pic}^0(\mathcal{X})$, then applying Riemann–Roch to $D + g\infty$ yields a function f such that $D + g\infty + \mathrm{div}(f) = D'$ is effective; so $[D' - g\infty] = [D]$ with $\deg D' = g$.

$D' - g\infty$ is *almost* a reduced representative:
it remains to remove any $P + \iota(P) - 2\infty = \mathrm{div}(x - x(P))$ from D'.

The Mumford representation

Suppose we have a class $[D]$ in $\mathrm{Pic}^0(\mathcal{X})(\Bbbk)$ with reduced representative

$$D = P_1 + \cdots + P_r - r\infty \in \mathrm{Div}^0(\mathcal{X})(\Bbbk) \ .$$

The **Mumford representation** of $[D]$ is the (unique) pair of polynomials $\langle a(x), b(x) \rangle$ in $\Bbbk[x]$ such that

- $a(x) = \prod_{i=1}^{r}(x - x(P_i))$, and
- $b(x(P_i)) = y(P_i)$ for $1 \leq i \leq r$;

for each of the x-coordinates appearing as a root of a, evaluating b gives the corresponding y-coordinate.

If necessary, compute b by Lagrange interpolation.

The Mumford representation

If $\langle a(x), b(x)\rangle$ represents a class on $\mathcal{X} : y^2 = f(x)$, then

1. a is monic of degree $r \leq g$, and
2. b satisfies $\deg b < r$ and $b^2 \equiv f \pmod{a}$.

Theorem: Any pair $\langle a(x), b(x)\rangle$ in $\mathbb{k}[x]^2$ satisfying these conditions represents a divisor class in $\mathrm{Pic}^0(\mathcal{X})(\mathbb{k})$.

$\implies$ identify divisor classes with Mumford reps of their reduced representatives: we simply write $[D] = \langle a, b\rangle$.

We associate $\langle a(x), b(x)\rangle$ *with the ideal* $(a(x), y - b(x))$.

We can collect the Mumford representations by degree $0 \leq d \leq g$:

$$M_d := \{\langle a, b\rangle : \deg(b) < \deg(a) = d, b^2 \equiv f \pmod{a}\} .$$

We can view the coefficients of $a(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ and $b(x) = b_{d-1}x^{d-1} + \cdots + b_0$ as coordinates on $\mathbb{A}^{2d}$.

$b^2 \pmod{a}$ and $f \pmod{a}$ are polynomials of degree $d - 1$ in $\Bbbk[a_i, b_i][x]$; the vanishing of their coefficients defines d independent equations in the $2d$ coordinates, cutting out M_d as a d-dimensional subvariety in $\mathbb{A}^{2d}$.

- M_0 is a point;
- M_1 is an affine copy of $\mathcal{X}$;
- $\#M_d(\mathbb{F}_q) = O(q^d)$ for $0 \leq d \leq g$.

Glueing together $M_0, \ldots, M_g$, we give $\mathrm{Pic}^0(\mathcal{X})$ the structure of a g-dimensional algebraic variety $\mathcal{J}_{\mathcal{X}}$, called the **Jacobian**.

Over $\mathbb{F}_q$, we have $\#\mathcal{J}_{\mathcal{X}} = O(q^g)$ *(more precision later)*.

We want an expression of the group law on $\mathcal{J}_{\mathcal{X}}$ in terms of its coordinates; Cantor's algorithm does this using an explicit form of Riemann–Roch.

Cantor's algorithm: addition on $\mathcal{J}_{\mathcal{X}}$

Input: Reduced divisors $D_1 = \langle a_1, b_1 \rangle$ and $D_2 = \langle a_2, b_2 \rangle$ on $\mathcal{X}$.
Output: A reduced $D_3 = \langle a_3, b_3 \rangle$ s.t. $[D_3] = [D_1 + D_2]$ in $\mathrm{Pic}^0(\mathcal{X})$.

1. $(d, u_1, u_2, u_3) := \mathrm{XGCD}(a_1, a_2, b_1 + b_2)$
   // so $d = \mathbf{gcd}(a_1, a_2, b_1 + b_2) = u_1 a_1 + u_2 a_2 + u_3(b_1 + b_2)$.
2. Set $a_3 := a_1 a_2 / d^2$;
3. Set $b_3 := b_1 + (u_1 a_1 (b_2 - b_1) + u_3 (f - b_1^2))/d \pmod{a_3}$;
4. If $\mathbf{deg}\, a_3 \leq g$ then go to Step 9;
5. Set $\tilde{a}_3 := a_3$ and $\tilde{b}_3 := b_3$;
6. Set $a_3 := (f - b_3^2)/a_3$;
7. Let $(Q, b_3) := \mathrm{Quotrem}(-b_3, a_3)$;
8. While $\mathbf{deg}\, a_3 > g$
   8a Set $t := \tilde{a}_3 + Q(b_3 - \tilde{b}_3)$;
   8b Set $\tilde{b}_3 := b_3$, $\tilde{a}_3 = a_3$, and $a_3 := t$;
   8c Let $(Q, b_3) := \mathrm{Quotrem}(-b_3, a_3)$;
9. Return $\langle a_3, b_3 \rangle$.

- Step 1: $d(x(P_i)) = 0$ iff $P_i = \iota(Q_j)$ for some j
- Steps 2, 3: sum D_1 and D_2, remove contribution of d $\longrightarrow$ pre-reduced D_3 such that $[D_3] = [D_1 + D_2]$
- Loop: reduces degree of the representative until reduced.
- Exercise: *how many steps until the result is reduced?*

Embeddings of Jacobians

The Mumford representation lets us compute with a hyperelliptic Jacobian by dividing it up into affine pieces:

$$\mathcal{J}_{\mathcal{X}} = M_0 \cup M_1 \cup \cdots \cup M_g \ .$$

In fact, $\mathcal{J}_{\mathcal{X}}$ is projective (it's an *abelian variety*)
—so what are its projective embeddings?